

日本国特許庁
JAPAN PATENT OFFICE

BSKB
(703) 205-8000
0397-041151
new
3/25/04
H. KUWAMURA
10/6

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年 3月28日

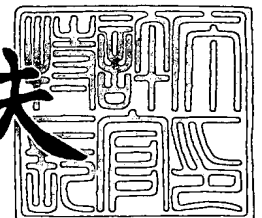
出願番号
Application Number: 特願2003-092095
[ST. 10/C]: [JP 2003-092095]

出願人
Applicant(s): シャープ株式会社

2004年 2月 4日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2004-3006157

【書類名】 特許願

【整理番号】 03J00087

【提出日】 平成15年 3月28日

【あて先】 特許庁長官殿

【国際特許分類】 H04M 1/00

【発明の名称】 個人認証機能付き携帯端末機器およびそのシステム

【請求項の数】 9

【発明者】

 【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内

 【氏名】 桑島 秀紀

【特許出願人】

 【識別番号】 000005049

 【氏名又は名称】 シャープ株式会社

【代理人】

 【識別番号】 100065248

 【弁理士】

 【氏名又は名称】 野河 信太郎

 【電話番号】 06-6365-0718

【手数料の表示】

 【予納台帳番号】 014203

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 0208452

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 個人認証機能付き携帯端末機器およびそのシステム

【特許請求の範囲】

【請求項 1】 通信基地局との双方向通信を行う通信機能を有する携帯端末機器であって、

個人認証情報を記憶する個人認証情報記憶部と、

携帯端末機器の使用者が正規の使用者であるのか否かを識別するための識別情報を入力する識別情報入力部と、

個人認証情報記憶部に記憶された個人認証情報に基づいて、識別情報入力部から入力された識別情報の個人認証を行う個人認証部と、

個人認証部による個人認証の結果、識別情報の個人認証が不成立であった場合には個人認証部の認証結果を通信基地局に通知する通知部を備えてなる個人認証機能付き携帯端末機器。

【請求項 2】 個人認証情報記憶部に記憶された個人認証情報が指紋情報からなり、

識別情報入力部が携帯端末機器の使用者の指紋を入力する指紋入力部からなり、

個人認証部が、個人認証情報記憶部に記憶された指紋情報に基づいて、指紋入力部から入力された指紋の個人認証を行う請求項 1 記載の個人認証機能付き携帯端末機器。

【請求項 3】 個人認証情報記憶部に記憶された個人認証情報が顔画像情報からなり、

識別情報入力部が携帯端末機器の使用者の顔を撮像するためのカメラからなり、

個人認証部が、個人認証情報記憶部に記憶された顔画像情報に基づいて、カメラで撮像された顔画像の個人認証を行う請求項 1 記載の個人認証機能付き携帯端末機器。

【請求項 4】 識別情報の個人認証が不成立であった場合にその認証不成立の結果を記憶する認証結果記憶部と、識別情報の個人認証が不成立であった場合

の制御を行う認証失敗制御部をさらに備え、

認証失敗制御部は、使用者から発信制御が行われたときに認証結果記憶部に記憶された認証不成立の結果が通信基地局に通知されるよう通知部を制御する請求項 1 記載の個人認証機能付き携帯端末機器。

【請求項 5】 識別情報の個人認証が不成立であった場合にその認証不成立の結果を記憶する認証結果記憶部と、識別情報の個人認証が不成立であった場合の制御を行う認証失敗制御部をさらに備え、

認証失敗制御部は、個人認証の不成立が所定の回数に達したときに認証結果記憶部に記憶された認証不成立の結果が通信基地局に通知されるよう通知部を制御する請求項 1 記載の個人認証機能付き携帯端末機器。

【請求項 6】 通知部により認証結果が通信基地局に通知された後、通信機能の一部または全部を停止する機能停止部をさらに備えてなる請求項 1 記載の個人認証機能付き携帯端末機器。

【請求項 7】 請求項 1 ～ 6 のいずれか 1 つに記載の携帯端末機器と、その携帯端末機器と双方向通信を行う通信基地局とからなる個人認証機能付き携帯端末機器システムであって、

通信基地局が、携帯端末機器の所有者の氏名、有線電話番号などの所有者情報を記憶する所有者情報記憶部と、携帯端末機器から識別情報の個人認証不成立の結果を受信するとその個人認証不成立の結果を所有者情報記憶部に記憶された所有者情報を参照して所有者に通知する認証結果所有者通知部を備えてなる個人認証機能付き携帯端末機器システム。

【請求項 8】 通信基地局が、携帯端末機器から識別情報の個人認証不成立の結果を受信するとその個人認証不成立の結果を所定の機関に通知する認証結果所定機関通知部をさらに備えてなる請求項 7 記載の個人認証機能付き携帯端末機器システム。

【請求項 9】 通信基地局が、識別情報の個人認証不成立の結果を受信したことを認証結果所有者通知部または認証結果所定機関通知部で通知する際、携帯端末機器と通信した通信基地局の位置情報を通知内容に含ませる位置情報付加部をさらに備えてなる請求項 7 または 8 記載の携帯端末機器システム。

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は、個人認証機能付き携帯端末機器およびそのシステムに関し、さらに詳しくは、携帯端末機器の盗難や紛失が発生した際の第三者による不正使用を防止する個人認証機能付き携帯端末機器およびそのシステムに関する。

【0002】**【従来の技術】**

近年、携帯電話やモバイル機器のような携帯端末機器の普及が進んでおり、利便性が一挙に拡大されてきている。しかし、一方では物理的な接続がなく、持ち運び可能であることから、盗難・紛失などの事態が発生する可能性もある。この場合、盗難・紛失などから第三者に渡った携帯端末機器は、携帯端末機器の所有者の意思に反して不正に使用される可能性がある。

【0003】

このような第三者の不正使用を防止するため、所有者が携帯端末機器の紛失に気がついた時点で、携帯端末機器の一部あるいはすべての機能を停止する、いわゆる携帯端末機器をロックする技術が知られている（例えば、特許文献1参照）。

【0004】

この技術では、携帯端末機器以外の通信装置からリモート操作で携帯端末機器の利用をロックするように制御することができる。この技術を用いることにより、紛失した携帯端末機器の第三者による不正使用を防止することができる。

【0005】

しかしこの技術は、所有者が携帯端末機器の盗難・紛失に気づいた後の対応を前提としている。したがって、携帯端末機器を紛失した時点から紛失に気がつくまでの間は、第三者による不正使用を防止することはできない。すなわち即時性のある対応はできない。

【0006】

そこで、この即時性を考慮した技術も開発されている（例えば、特許文献2参

照)。図8にこの従来技術における携帯端末機器のシステム構成図を示す。

この技術では、携帯端末機器31とは別に、携帯端末機器31に対応した位置登録端末機器32をあらかじめ用意しておく。そして、携帯端末機器31と共に、位置登録端末機器32も通信基地局33に随時、位置情報を通知する。もし、携帯端末機器31と位置登録端末機器32の距離が一定距離以上離れば、通信基地局33から所有者にその情報を通知する。この手法により、携帯端末機器の盗難・紛失を早急に検知できるため、携帯端末機器の所有者は、この通知をもって速やかに通信基地局に対して、携帯端末機器のロックを行うように手続きすることで、第三者の不正使用を防止することができる携帯端末機器システムを提案している。

【0007】

【特許文献1】

特開平6-125305号公報

【特許文献2】

特開平9-191342号公報

【0008】

【発明が解決しようとする課題】

しかしながら、携帯端末機器とは別に位置登録端末機器も一緒に持ち運ぶようにした場合には、携帯としての利便性を損ねてしまう。昨今の携帯端末機器は小型軽量化が重要なテーマになっており、この点は大きなマイナス要素である。

【0009】

また、消費電力との兼ね合いもあるが、携帯端末機器、位置登録端末機器共に、可能な限り位置登録情報を更新したとしても、紛失した携帯端末機器の不正使用の場所が同一通信基地局内であれば、この不正使用を防止することができない。

【0010】

本発明は、このような事情を考慮してなされたもので、携帯端末機器に個人認証の機能を設けることで、盗難や紛失によって第三者の手に渡った携帯端末機器の第三者による不正使用を防止することを目的とするものである。

【0011】**【課題を解決するための手段】**

本発明は、通信基地局との双方向通信を行う通信機能を有する携帯端末機器であって、個人認証情報を記憶する個人認証情報記憶部と、携帯端末機器の利用者が正規の利用者であるのか否かを識別するための識別情報を入力する識別情報入力部と、個人認証情報記憶部に記憶された個人認証情報に基づいて、識別情報入力部から入力された識別情報の個人認証を行う個人認証部と、個人認証部による個人認証の結果、識別情報の個人認証が不成立であった場合には個人認証部の認証結果を通信基地局に通知する通知部を備えてなる個人認証機能付き携帯端末機器である。

【0012】

本発明によれば、識別情報入力部から個人認証用の識別情報が入力されると、あらかじめ記憶された個人認証情報に基づいて、入力された識別情報の個人認証が行われる。その結果、識別情報の個人認証が不成立であった場合には、その認証結果が通信基地局に通知される。通信基地局では、その結果に基づいて、該当する携帯端末機器の使用を制限したり、有線電話で所有者に連絡するなど、各種の対策を講ずることが可能となり、これにより、所有者が携帯端末機器の盗難や紛失に気づいていない場合でも、第三者による不正使用を確実に防止することができる。

【0013】**【発明の実施の形態】**

本発明において、個人認証情報記憶部は、個人認証を行うことが可能な情報を記憶できるものであればよく、当該分野で公知の各種の半導体メモリ、磁気記録媒体、光学式記憶媒体などを適用することができる。この個人認証情報記憶部は、小型の携帯端末機器に内蔵可能なものであることが望ましく、その点からはデジタルカメラの記憶媒体などに用いられているカード式メモリなどを適用することが望ましい。

【0014】

識別情報入力部は、携帯端末機器の利用者が正規の利用者であるのか否かを識

別するための識別情報を入力できるものであればよく、当該分野で公知の各種の入力装置を適用することができる。

【 0 0 1 5 】

この識別情報入力部は、携帯端末機器の使用者の指紋を入力する指紋入力部で構成されていてもよい。指紋入力部としては、指紋センサに指を置いたときに、センサ内の電荷の量から指紋の形を判定する半導体式指紋センサなどを適用することができる。また、識別情報入力部は、携帯端末機器の使用者の顔を撮像するためのカメラで構成されていてもよい。カメラとしては、携帯端末機器に内蔵可能な小型の C C D カメラなどを適用することができる。

【 0 0 1 6 】

識別情報入力部を指紋入力部で構成する場合には、個人認証情報記憶部には個人認証情報として指紋情報を記憶させておき、指紋センサで検出した指紋情報を個人認証情報記憶部の指紋情報と比較して個人認証を行う。また、識別情報入力部をカメラで構成する場合には、個人認証情報記憶部には個人認証情報として顔画像情報を記憶させておき、カメラで撮影された顔画像情報を個人認証情報記憶部の顔画像情報と比較して個人認証を行う。

【 0 0 1 7 】

個人認証部は、個人認証情報記憶部に記憶された個人認証情報に基づいて、識別情報入力部から入力された識別情報の個人認証を行うことができるものであればよい。この個人認証部としては、プログラムで作動可能な各種のプロセッサを適用することができる。このプロセッサは、携帯端末機器のプロセッサを適用したものであってもよいし、携帯端末機器とは別のプロセッサを用いたものであってもよい。

【 0 0 1 8 】

通知部は、個人認証部による個人認証の結果、識別情報の個人認証が不成立であった場合にはその認証結果を通信基地局に通知できるものであればよく、当該分野で公知の各種の情報送信装置を適用することができる。この通知部としては、携帯端末機器に内蔵した通常の情報送信に利用する情報送信装置を適用することが望ましい。

【0019】

以下、図面に示す実施の形態に基づいてこの発明を詳述する。なお、この発明はこれによって限定されるものではなく、各種の変形が可能である。

【0020】

図1は本発明の個人認証機能付き携帯端末機器システムの構成を示すブロック図である。本携帯端末機器システムは携帯端末機器1と通信基地局20とで構成される。

【0021】

携帯端末機器1は、携帯電話やモバイル機器からなり、無線部2、通信制御部3、システム制御部4、個人認証部5、メモリ部6、キー入力部7、表示部8、音声処理部9、カメラ部10、認証失敗制御部11、認証失敗情報記録部12、認証失敗情報通知部13、および機能停止部14から構成されている。

【0022】

通信基地局20は、位置情報記憶部21と所有者情報記憶部22とを有している。また、通信基地局20には、携帯電話以外の例えば有線電話などにより携帯電話の所有者と連絡をとるための別連絡部23と、警察署に連絡をとるための警察署連絡部24とが設けられている。

【0023】

無線部2は、通信基地局20との間で無線回線を通じて、通信を行うための電波信号と電気信号をお互い変換する機能を有している。

通信制御部3は、通信を実現するための、いわゆるベースバンド処理回路であり、一般にはモデム機能やチャネルコーディック機能から実現される。

【0024】

例えば、電波信号受信時、モデムには、通信基地局20から送られてきた電波信号が、無線部2を介することにより、電気信号（アナログ信号）として変換され、入力される。

【0025】

モデムは、受信したアナログ信号をデジタル信号に変換して（いわゆる復調）、後段のチャネルコーディックにデジタル信号情報を渡す。チャネルコーディッ

クは、このデジタル信号情報に対して、通信の規格で定められた特定のデジタル処理を行う。なお、本例におけるチャネルコーディックは、音声情報信号とシステム制御信号の分離、結合を行う機能も備えているものと定義する。特定のデジタル処理が終了したら、音声情報信号とシステム制御信号を分離して、音声情報信号は音声処理部 9 へ、システム制御信号はシステム制御部 4 へそれぞれ渡す。

【 0 0 2 6 】

また、電波信号送信時には、チャネルコーディックはシステム制御部 4 からのシステム制御信号と、音声処理部 9 からの音声情報信号とを結合、さらに、特定のデジタル処理を行ったのち、モデムへ送信デジタル信号として渡す。

モデムは、このデジタル信号をアナログ信号に変換し（変調）、無線部 2 を介することで電波信号とし、通信基地局 2 0 へ信号を送出する。

【 0 0 2 7 】

通信プロトコルに則する必要な信号のやり取りが通信基地局 2 0 と正常に行われることにより、携帯端末機器 1 は通信基地局 2 0 と通信できる、いわば接続された状態となる。

【 0 0 2 8 】

システム制御部 4 は、いわゆるマイコンや、マイコンが作業を行うため必要な一時記憶部などから構成され、携帯端末機器 1 のシステム全体の制御を行う。

システム制御部 4 には、携帯端末機器 1 の使用者が正規な使用者（以下、正規ユーザーと記載する）かどうかの個人認証を行うことができる個人認証部 5、電話アドレス情報やメールなどの情報を記憶しておくメモリ部 6、携帯端末機器へ情報を入力するためのキー入力部 7、個人情報やシステムの状態などを表示する表示部 8、個人認証失敗時にあらかじめ定めておいた処理を携帯端末機器で行うように制御する認証失敗制御部 1 1、およびカメラ 1 0 が接続されている。

【 0 0 2 9 】

個人認証部 5 は、番号の組み合わせ等のいわゆるパスワードではなく、指紋や顔情報のような生体情報から個人認証を行う、いわゆるバイオメトリクス認証技術を適用したものである。これは、利便性や、セキュリティのレベルの向上に大きく貢献する。具体的な個人認証の手段としては、本例では指紋認証技術を用い

ている。これに代えて、カメラ 1 0 などを使用しての顔認証技術を用いてもよい。

【0 0 3 0】

指紋認証技術には、指紋センサに指を置いたときに、センサ内の電荷の量から指紋の形を判定する半導体式指紋認証方式など、いくつかの手法があるが、本例では特にこだわらない。

【0 0 3 1】

したがって、個人認証部 5 は、指紋情報を読み取る指紋センサ、特別な正規ユーザー登録方法で正規ユーザーの指紋データを登録、格納するメモリ、指紋センサで読み取られた指紋データと、登録してある正規ユーザーの指紋データとを比較して、正規ユーザーとして識別できるかどうか判断する比較器を備えている。比較器から出力される個人認証結果情報は、認証失敗制御部 1 1 に送られる。

【0 0 3 2】

携帯端末機器 1 は、所有者だけでなく、複数の人数で使用するケースも考えられる。この場合、こちらも特別な正規ユーザー登録方法で、新規ユーザーの指紋データを追加登録してもよい。特別な正規ユーザー登録方法とは、処理フローの説明時に記載（後述）する。

【0 0 3 3】

メモリ部 6 は、携帯端末機器のいわゆるプログラムを格納している R O M や、電話アドレス情報や、メールなどの情報を記憶しておくことができる F R O M などから構成されており、必要に応じてシステム制御部 4 との間で情報の読み出しや書き込みが行われる。

【0 0 3 4】

キー入力部 7 は、テンキーや各種モードキーなどから構成されており、携帯端末機器の使用者のキー操作を入力情報として、システム制御部 4 に渡す。

表示部 8 は、ドットマトリクス構成の液晶パネルおよび各ドライバなどから構成され、キー入力部 7 から入力された番号などの情報画像や、各種通信モードを表す画像、電話機能の動作状態を示すアイコン画像等、携帯端末機器としての必要な情報が、システム制御部 4 からの指示により適宜表示される。

【0035】

音声処理部 9 は、音声情報信号から実際の音声に変換するための D/A コンバータ、フィルタ、スピーカなどを備え、通信制御部 3 から入力された音声情報を、携帯端末機器の外に実際の音声として出力する。また、実際の音声マイクから入力されたら、A/D コンバータ、フィルタなどを用いて、音声処理を行った後、音声情報信号（デジタル信号）を通信制御部 3 に渡す機能を備える。

【0036】

認証失敗制御部 11 は、個人認証失敗時に、携帯端末機器 1 に対してどのような処理を行うかをまとめたブロックであり、認証失敗情報記録部 12、認証失敗情報通知部 13、機能停止部 14 と接続される。

【0037】

認証失敗情報記録部 12 は、個人認証を何回失敗、あるいは成功したかを記憶する。なお、本例では個人認証部 5 やメモリ部 6 とは別に記載しているが、これらに含まれていてもよい。

携帯端末機器 1 の構成は上記のとおりである。

【0038】

携帯端末機器 1 の使用契約時には、あらかじめ通信基地局 20 を管理する通信キャリア側へ、正規ユーザーの緊急連絡先などの所有者情報を登録しておく。この所有者情報は所有者情報記憶部 22 に記憶されている。通信キャリア側は、携帯端末機器 1 以外の例えば有線電話などで正規ユーザーに連絡をとるための別連絡部 23 を有しており、この別連絡部 23 を用い、所有者情報記憶部 22 を参照することで、正規ユーザーに連絡することができるようになっている。なお、携帯端末機器の使用契約時と記載したが、もちろんこの時点のみではなく、携帯端末機器システムの適用開始時までに所有者情報を登録すればよい。図 7 に所有者情報の一例を示す。

【0039】

以下、上述のように構成された携帯端末機器システムの動作について説明する。最初に、一般的な携帯端末機器の処理フローの一例を図 2 に示す。

まず、キー入力部 7 による携帯端末機器 1 の電源 ON 操作が行われると、携帯

端末機器起動処理が行われる（ステップ S 1）。この処理は、携帯端末機器自体の起動処理の他、セルサーチ等、通信プロトコルに即した所定の処理も含む。この所定の手続きにより、通信基地局 2 0 との交信を開始し、通信可能な状態に進む（ステップ S 2）。これを本例では待機状態と記載する。

【 0 0 4 0 】

また、待機状態であることを使用者に報知するため、表示部 8 に適切な情報を表示してもよい。たとえば、携帯端末機器に一般的に内蔵されている時計機能から、現在の時刻を表示する。一般的に、携帯端末機器はこの待機状態のまま使用される。

【 0 0 4 1 】

携帯端末機器 1 は待機状態である中、使用者のキー操作によって、なんらかの処理要求を受け付けいたら（ステップ S 3）、要求に対応した処理を行う（ステップ S 4）。この処理を本例では通常処理と記載する。通常処理とは、たとえば、通話を開始するように操作されたら、システム制御部 4 は、例えば通信制御部 3、無線部 2、音声処理部 9 など通話に必要な機能を用いて通話を行う。また、アドレス情報を表示させるような要求を受け付けいたら、システム制御部 4 は、メモリ部 6 から必要なデータを読み出し、表示部 8 に表示させる。通常処理とは、このような一般的な携帯端末機器の処理のことである。

【 0 0 4 2 】

さらに、待機状態である中で、キー入力部 7 から電源 O F F 操作を受け付けいたら（ステップ S 5）、システム制御部 4 は、携帯端末機器の O F F 処理を行い、電源を切る（ステップ S 6）。

【 0 0 4 3 】

以上が一般的な携帯端末機器の利用形態である。次に、本発明における正規ユーザー登録処理について記載する。図 3 に正規ユーザー登録処理のフローを示す。

携帯端末機器 1 が待機状態であるときに（ステップ S 2）、正規ユーザー登録処理を行うように操作すると（ステップ S 7）、携帯端末機器 1 は正規ユーザー登録処理に進む（ステップ S 8）。特に携帯端末機器 1 を新規に使用する場合で

あれば、この処理を行う必要がある。

【0 0 4 4】

以下、ステップ S 8 の正規ユーザー登録処理について記載する。ここに記載する正規ユーザー登録とは、個人認証処理を行うための前準備であり、さらに個人認証処理とは、携帯端末機器 1 を操作している使用者が、正規ユーザーであるのか、あるいは不正に使用しようとしている第三者であるのかを、識別、認証する処理のことである。本発明において、この個人認証処理は幾度となく繰り返し実行されることになるので、本処理の操作の利便性は大変重要な課題である。したがって、高度なセキュリティを保ちつつ、かつ利便性を考慮すると、いわゆる煩雑なパスワード入力などではなく、指を指定の場所に置くだけなどの簡易な操作で認証手続きが実行できる指紋認証技術など用いることが望ましい。

【0 0 4 5】

正規ユーザー登録を行う際には、第三者によって容易に登録されることを禁止するため、特別な手法をもって行う。「特別な」とは、第三者が容易に推測、実現できない、複雑な手法のことである。たとえば、長いパスワードを用いてもよいし、携帯端末機器 1 とは別の端末機器を用意して、これと接続しながらではないと正規ユーザー登録を行えないようにしてもよい。長いパスワードや別の端末機器は、常に携帯端末機器と一緒に携帯しておく必要はないが（逆に、容易な携帯性がないほうが望ましい）、所有者はこのパスワードや別の端末機器をきっちりと管理することが重要である。このように正規ユーザー登録処理は、利便性を犠牲にしたほうが、かえってセキュリティの向上につながる。

【0 0 4 6】

具体的には、まず、携帯端末機器 1 に、上述した特別な手法でもって、現在の携帯端末機器の使用者が正規ユーザーであることを認証させる。次に、個人認証部 5 から正規ユーザーの指紋データを読み取り、そのデータを正規ユーザーの指紋データとして、メモリに格納する。このメモリは携帯端末機器 1 のメモリ部 6 を使用してもよいし、個人認証部 5 内に別途備えておいてもよい。ただし、携帯端末機器 1 の電源が OFF されても、正規ユーザー登録情報は記憶し続けるものとする。こうしないと、利便性が著しく低下してしまう。正規ユーザー登録処理

が完了すれば、携帯端末機器 1 の待機状態であるステップ S 2 に戻る。

【0047】

なお、複数の人間が本携帯端末機器 1 を共有して使用するケースも考えられる。この場合は、最初に正規ユーザーとして登録した人の了解のもと、いわば正規ユーザーが携帯端末機器 1 の管理者としてふるまい、具体的には上記のような特別な手法を用いて新規に正規ユーザーを追加する。

【0048】

次に、本発明における正規ユーザーの個人認証機能有効処理について記載する。図 4 に正規ユーザーの個人認証機能有効処理のフローを示す。

正規ユーザーが、携帯端末機器 1 が待機状態であるときに（ステップ S 2）、すでに正規ユーザー登録処理が行われていれば、個人認証機能を有効あるいは無効にするように操作すると（ステップ S 9）、携帯端末機器 1 は個人認証機能有効処理に進む（ステップ S 10）。個人認証機能有効とは、携帯端末機器の使用者が、登録してある正規ユーザーであることを識別、認証した結果でもって、各種通常処理の動作可否を制御するかどうか選択するフラグ（イネーブル）情報である。この情報も、携帯端末機器 1 の電源が OFF されても記憶し続けるものとする。なお、本発明では、個人認証機能は有効であるのが前提ではあるが、もちろんこのステップ S 10 でその機能を一時的に OFF にすることも選択できる。

【0049】

次に、本発明の主旨である個人認証機能が有効である場合の携帯端末機器 1 の動作について記載する。図 5 に個人認証機能が有効である場合の処理フローを示す。

一般に、携帯電話などの携帯端末機器は、利便性から、通常は、ステップ 2 の待機状態で使用されるケースがほとんどである。本例では、図 3 におけるステップ S 8 で、正規ユーザーの登録処理を行っている携帯端末機器 1 の動作が、ステップ S 2 の待機状態であるとして、以下記載する。

【0050】

ここで、携帯端末機器 1 の使用者が、キー入力部 7 から通常処理を行うよう操作すると（ステップ S 3）、システム制御部 4 は、要求された通常処理を行う際

に、個人認証が必要かどうか判断し、もし必要のない通常処理の要求ならば、ステップS4の通常処理を直接実行してもかまわない。すなわち、ここで記載した通常処理とは、セキュリティをかける必要のない処理であり、たとえばカレンダー表示やゲームなどが考えられる。このように各通常処理別に、個人認証が必要かどうかを設定できるようにしておくと、正規ユーザーとして登録されていない第三者でも、図4におけるステップS10で個人認証機能の設定変更を行わずに通常処理を利用できるようになるため、利便性が向上する。

【0051】

ステップS3で、個人認証が必要な通常処理の実行要求があった場合には、図4におけるステップS10で、個人認証機能が有効に設定されているか調べる（ステップS11）。そもそも個人認証機能が有効でない場合では、ステップS4の要求された通常処理を行う。しかし、個人認証機能が有効である場合は個人認証処理（ステップS12）に進む。個人認証処理は、携帯端末機器1を使用する際に、第三者の不正利用を防止し、正規ユーザーだけ正しく使用できるよう制御するステップである。ステップS12に進んだときは、要求された通常処理を行うには、個人認証が必要であることを示す情報を表示部8に表示してもよい。

【0052】

個人認証処理は、まず携帯端末機器1の使用者に、認証部5を使用して使用者の指紋情報を入力させる。つぎに、個人認証部5内で、入力された指紋情報が、あらかじめ図3におけるステップS8で正規ユーザーとして登録してある指紋情報と一致するか、比較器などを用いて照合、識別する。識別した結果、正規ユーザーか、あるいは登録していない第三者かの情報（個人認証結果情報）を、認証失敗制御部11に送る。

【0053】

この段階で、識別した結果が正規ユーザーのものであれば、ステップS4に進んで、要求された通常処理を行うが、もし、登録されていない第三者のものであれば、認証失敗制御部11は認証失敗情報通知部13を使用して、通信基地局20に、認証失敗が発生したことを知らせる認証失敗情報を発信、通知する（ステップS13）。

【 0 0 5 4 】

このとき、認証失敗制御部 1 1 は、一度だけの認証結果から、認証失敗と判断するのではなく、たとえば 5 回連続で認証に失敗するなど、複数回認証に失敗した時点で初めて認証失敗とみなしてステップ S 1 3 に進んでもよい。この場合、認証に失敗した回数を認証失敗情報記憶部 1 2 に記憶させておく必要がある。何回認証に失敗すれば認証失敗とみなすのかは、携帯端末機器 1 の使用者が任意に設定できるものとする。

【 0 0 5 5 】

また、認証失敗とみなしても、この状態をすぐ通信基地局 2 0 に通知することせず、認証失敗状態であることを記憶しておき、この状態の携帯端末機器 1 から発信の実行が操作された時に、初めて認証失敗情報を基地局に通知するようにしてもよい。

【 0 0 5 6 】

上記のような、複数回の認証確認後に初めて認証失敗の処理を行うことや、発信制御が行われようとしたときに初めて認証失敗の処理を行うことは、おもに誤作動（意図しない連絡）を防ぐことを目的としている。

【 0 0 5 7 】

たとえば、所有者が、認証失敗情報が通信基地局 2 0 に連絡されることなど意図せず、ただ単に携帯端末機器 1 に格納している情報を知人に見せようとして、同機を手渡す場合などが考えられるが、このときでも、いきなり認証失敗、即通知では、通知する基地局側に負荷がかかる。また、所有者側にも必要ない情報が連絡されることになり、利便性が損なわれてしまう。

【 0 0 5 8 】

認証失敗と判断した認証失敗制御部 1 1 は、認証失敗情報通知部 1 3 に対して通信基地局 2 0 へ向け、認証失敗情報を通知するよう要求を出力する。認証失敗情報通知部 1 3 は、携帯端末機器 1 の使用者の操作に関わらず、通信（発信）に必要な機能、すなわち通信制御部 3 を用いてその情報を通信基地局 2 0 側に通知する。

【 0 0 5 9 】

また、認証失敗制御部 11 は、認証失敗と判断したら、携帯端末機器 1 の一部あるいはすべての機能を制限する、いわゆるロック処理を行ってもよい（ステップ S14）。

【0060】

まず、携帯端末機器 1 にあらかじめ、認証失敗情報を受け付けた場合、すなわち携帯端末機器 1 が第三者に不正に使用されようとしていると考えられた場合、携帯端末機器 1 にどのような機能制限を行うか設定しておく（不図示）。ここで述べる機能制限とは、携帯端末機器 1 が不正使用されないように、例えば、勝手に通信されないように通信制御部 3 の動作を停止させたり、メモリ部 6 の内容を閲覧されないようにしておいたりすることである。機能停止部 14 は、認証失敗制御部 11 から認証失敗情報を受け付けたら、設定されている上記情報に基づき携帯端末機器 1 のロックを行う。

【0061】

たとえば、通常処理 4 に含まれる通話機能や、アドレス表示機能などの機能をロック（使用できない）するようにする。さらに、この情報を表示部 8 に表示してもよい。この制御によって、携帯端末機器 1 が不正使用される前に、確実に即時性をもって携帯端末機器の不正使用を防止することができる。

【0062】

以下、認証失敗情報を受け取った通信基地局側 20 の処理フローを図 6 に記載する。図 5 のステップ S13 で発信された認証失敗情報を受信した通信基地局 20 は（ステップ S15）、事前に所有者情報記憶部 22 に登録してある所有者情報を参照して、携帯端末機器 1 とは別の別連絡部 23 でもって、所有者に認証失敗情報を通知する（ステップ S16）。このため、正規ユーザーは紛失、盗難などの発生情報を、即時性をもって得ることができる。また、認証失敗情報を所有者に通知するさいに、位置情報記憶部 21 に記憶した通信基地局 20 の位置情報を付加してもよい。こうしておけば、紛失した携帯端末機器 1 の位置情報がわかるため、所有者は携帯端末機器 1 がどこにあるか、見つけやすくなる効果が得られる。また、単なる紛失ではなく、第三者による盗難かどうかの判断材料のひとつにもなる。

【0063】

なお、よりセキュリティの向上のため、認証失敗情報を受け付けたら、警察署連絡部 2 4 により（ステップ S 1 7）、警察署に通知してもよい（ステップ S 1 8）。この警察署へ通知をするか否かは、基本的に携帯端末機器 1 の正規ユーザーが設定できるようにしておく。また、いつでもその設定を変更できるようにしておく。もし警察署への連絡が必要なければ、通信基地局 2 0 側にそのように設定をしておくこともできる。

【0064】

このようにして、携帯端末機器に個人認証の機能を設けることにより、盗難や紛失によって第三者の手に渡った携帯端末機器の第三者による不正使用を防止することができる。

【0065】**【発明の効果】**

本発明によれば、携帯端末機器が盗難や紛失により第三者の手に渡った場合でも、第三者による不正使用を確実に防止することができる。また、即時性を持った情報が通信基地局から得られるため、盗難や紛失の発生を正規ユーザーが速やかに知ることができる。さらに、この情報に通信基地局の位置情報が含まれていれば、紛失した携帯端末機器を探す手がかりになり、紛失か盗難かの判断材料とすることができる。

【図面の簡単な説明】**【図 1】**

本発明の個人認証機能付き携帯端末機器システムの構成を示すブロック図である。

【図 2】

実施形態における携帯端末機器の基本動作状態を示すフローチャートである。

【図 3】

実施形態における携帯端末機器の正規ユーザー登録処理を示すフローチャートである。

【図 4】

実施形態における携帯端末機器の個人認証機能有効処理を示すフローチャートである。

【図 5】

実施形態における携帯端末機器の個人認証機能を用いた処理を示すフローチャートである。

【図 6】

実施形態における通信基地局側の処理を示すフローチャートである。

【図 7】

実施形態における通信基地局側の所有者情報の一例である。

【図 8】

従来例における携帯端末機器のシステム構成図である。

【符号の説明】

- 1 携帯端末機器
- 2 無線部
- 3 通信制御部
- 4 システム制御部
- 5 個人認証部
- 6 メモリ部
- 7 キー入力部
- 8 表示部
- 9 音声処理部
- 10 カメラ
- 11 認証失敗制御部
- 12 認証失敗情報記録部
- 13 認証失敗情報通知部
- 14 機能停止部
- 20 通信基地局
- 21 位置情報記憶部
- 22 所有者情報記憶部

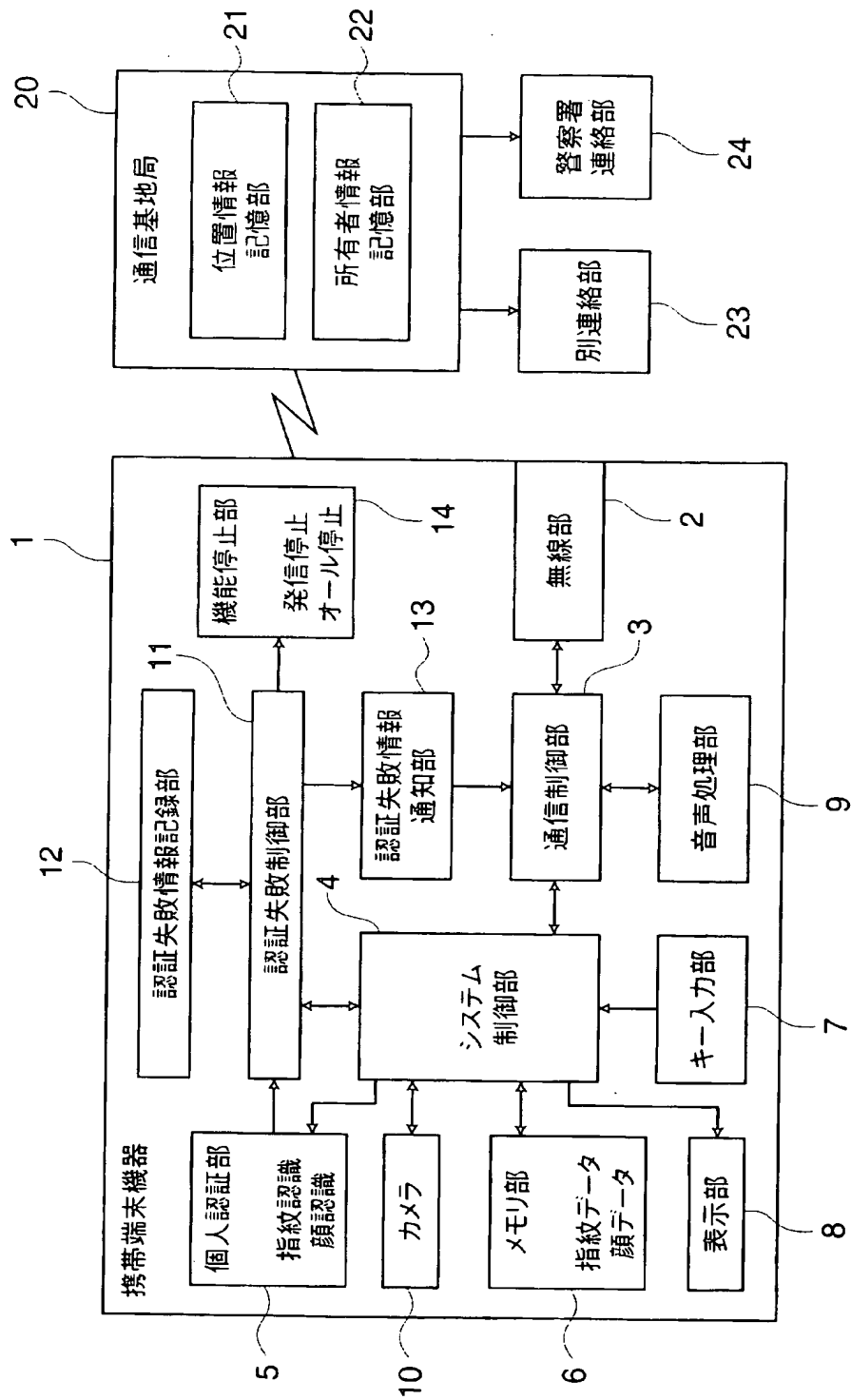
2 3 別連絡部

2 4 警察署連絡部

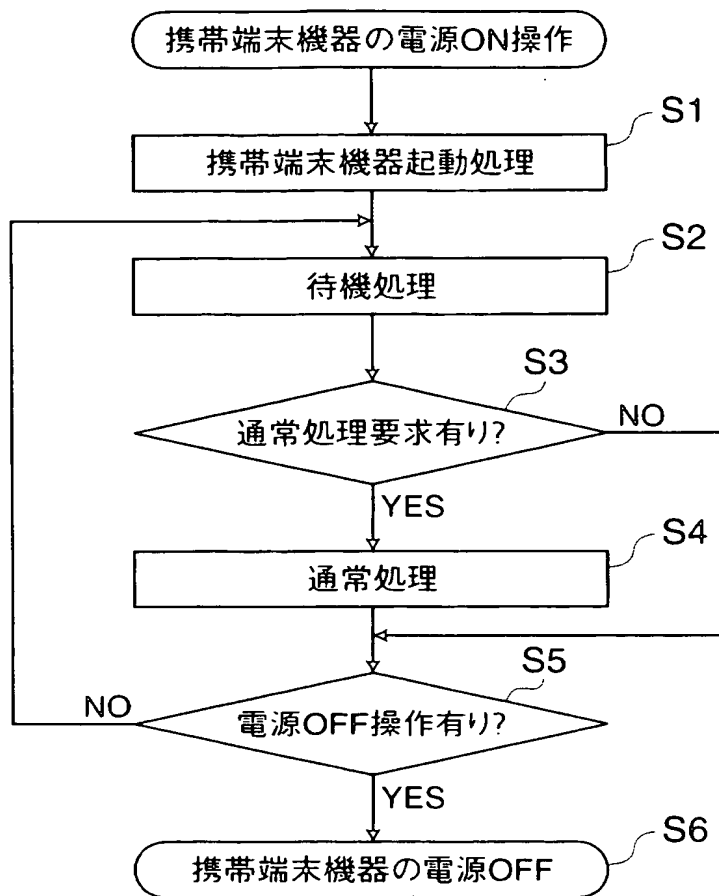
【書類名】

図面

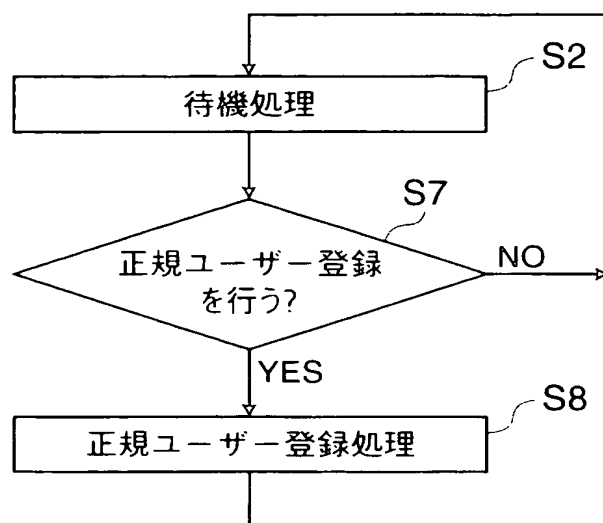
【図 1】



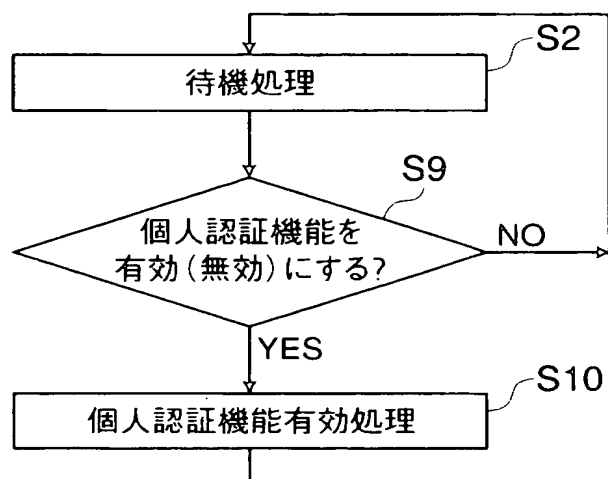
【図 2】



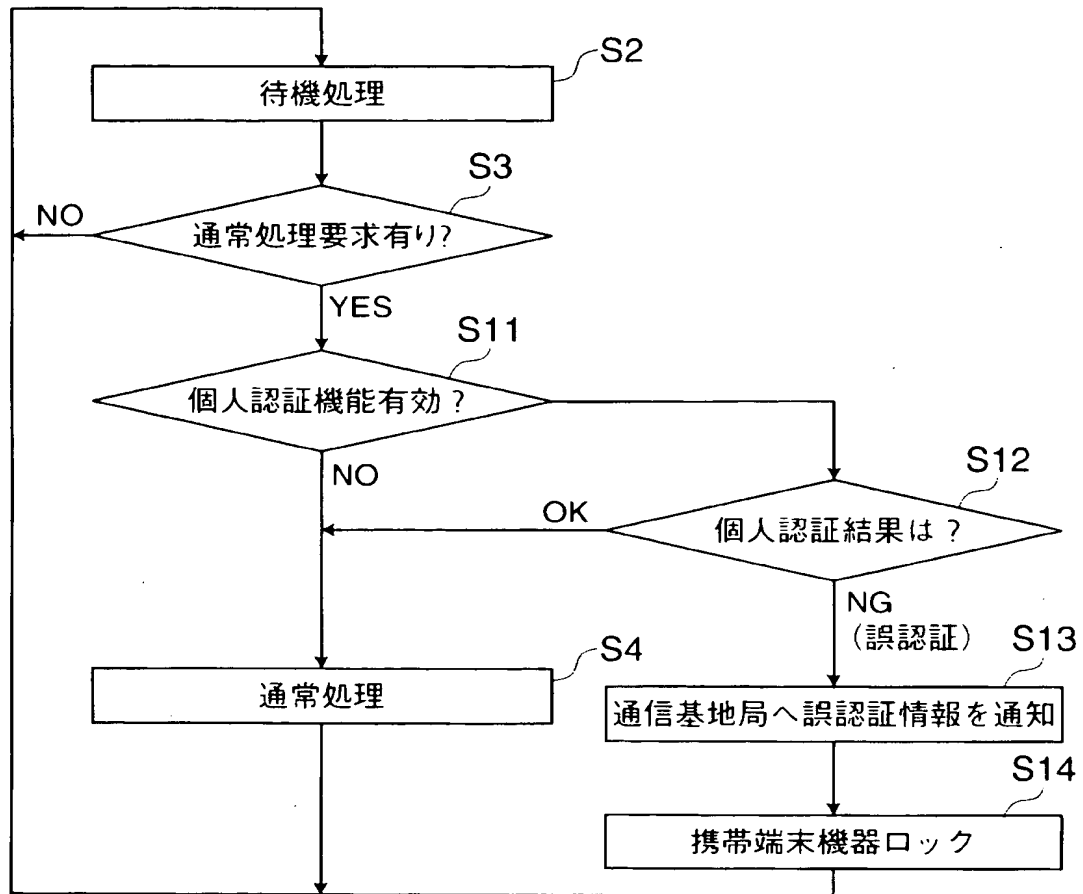
【図 3】



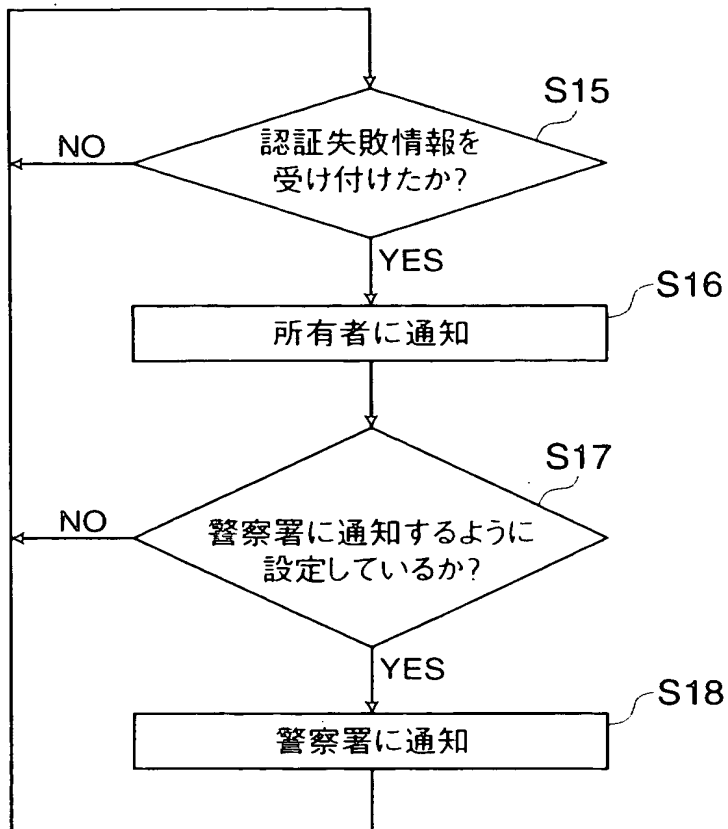
【図 4】



【図 5】



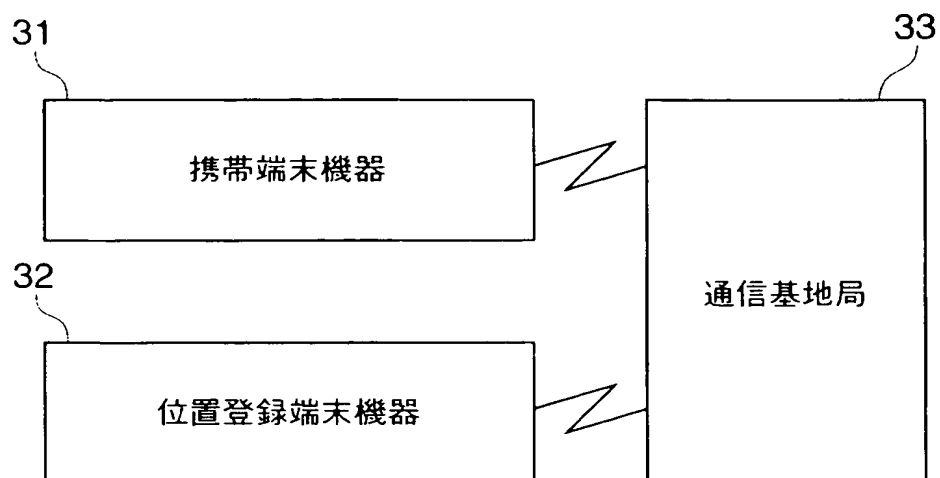
【図 6】



【図 7】

ID	01234567
氏名	〇〇 ××
携帯端末機器連絡番号	090-XXXX-XXXX
緊急連絡先	奈良県大和郡山市XX町XX
別連絡部の連絡番号	0743-XX-XXXX
最新通話(受信)時間	20XX/XX/XX XXhXXmXXs
認証失敗情報受信時間	20XX/XX/XX XXhXXmXXs

【図 8】



【書類名】 要約書

【要約】

【課題】 携帯端末機器に個人認証の機能を設けることで、盗難や紛失によって第三者の手に渡った携帯端末機器の第三者による不正使用を防止する。

【解決手段】 携帯端末機器に、正規ユーザーの指紋情報を記憶した指紋情報メモリと、指紋センサとを設け、プロセッサにより、指紋センサで読み取った指紋情報が指紋情報メモリに記憶した正規ユーザーの指紋情報と一致するか否かを判定し、不一致であった場合にはその結果を通信基地局に通知する。

【選択図】 図 1

特願 2 0 0 3 - 0 9 2 0 9 5

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 0 4 9]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

大阪府大阪市阿倍野区長池町 2 2 番 2 2 号

氏 名

シャープ株式会社